Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та управління

Кафедра інформаційної та кібернетичної безпеки

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ О.Б.Жильцов
«_11_» ____09____ 2018 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ ТА КОДУВАННЯ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 0944/18
(підпис) (прізвище, ініціали)
«___» _____ 2018 р.

Київ – 2018

Розробники:

Астапеня Володимир Михайлович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Аносов Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Викладач:

Астапеня Володимир Михайлович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки

Протокол від 13.09.2018 р. № 6

Завідувач кафедри _____ (підпис) В.Л. Бурячок

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 20___ р.

Керівник освітньої програми _____ (підпис) (В.В. Семко)

Робочу програму перевірено

___.___. 20___ р.

Заступник директора/декана _____ (підпис) І.Ю. Мельник

Пролонговано:

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	нормативна	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4 / 120	
Курс	3	
Семестр	5	
Кількість змістових модулів з розподілом:	4	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	56	
Модульний контроль	8	
Семестровий контроль		
Самостійна робота	56	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Основи захисту інформації та кодування» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека, освітньої програми 125.00.01 «Безпека інформаційних і комунікаційних систем».

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач другого (магістерського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Основи захисту інформації та кодування» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Основи захисту інформації та кодування» складається з чотирьох змістових модулів: Загальні питання перетворення інформації; Принципи та методи надання доступу до інформаційних ресурсів; Основи теорії кодування; Основні стандарти та механізми криптографічного захисту інформації Обсяг дисципліни – 120 год. (4 кредити).

Метою викладання навчальної дисципліни «Основи захисту інформації та кодування» є формування у студентів знань про фізичні процеси, що відбуваються при перетворенні інформації у електронних пристроях, вмінь застосувати основні стандарти та механізми криптографічного захисту інформації для забезпечення безпеки в інформаційно-телекомунікаційних (автоматизованих) систем

Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері інформаційної та кібернетичної безпеки та набуття **наступних компетентностей**:

Фахові компетентності

КФ-10: Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

знати:

- основи теорії інформації та сучасні напрямки її розвитку;
- основи теорії сигналів, спектрального аналізу та цифрової обробки сигналів;
- принципи кодування інформації в аналого-цифрового та цифро-аналогового перетворювачах;
- основи теорії кодування інформації та їх застосування в інформаційній техніці.;
- методи аналізу сигналів і їх основних характеристик;
- основи аналізу дискретних сигналів з розподіленими параметрами.

уміти:

- використовувати сучасні методи теорії інформації та кодування в інформаційних системах;
- проводити дослідження аналого-цифрових перетворювачів;
- досліджувати моделі системи передачі даних із використанням циклічного коду;
- проводити дослідження роботи модуляторів-демодуляторів;
- застосувати основні стандарти та механізми криптографічного захисту інформації.

та досягти наступних **програмних результатів навчання:**

ПРз-10: аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації; аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації; виявляти небезпечні сигнали технічних засобів; вимірювати параметри небезпечних та завадових сигналів під час інструменттального контролю захищеності інформації від витоку технічними каналами; визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації; інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації; обґрунтовувати можливість створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Загальні питання перетворення інформації							
Тема 1. Загальні питання перетворення інформації	28	6		4	4		14
Модульний контроль	2						
Разом	30	6		4	4		14
Змістовий модуль 2. Принципи та методи надання доступу до інформаційних ресурсів							
Тема 2. Принципи та методи надання доступу до інформаційних ресурсів	28	6		4	4		14
Модульний контроль	2						
Разом	30	6		4	4		14
Змістовий модуль 3. Основи теорії кодування							
Тема 3. Основи теорії кодування	28	6		4	4		14
Модульний контроль	2						
Разом	30	6		4	4		14
Змістовий модуль 4. Основні стандарти та механізми криптографічного захисту інформації							
Тема 4. Основні стандарти та механізми криптографічного захисту інформації	28	6		4	4		14
Модульний контроль	2						
Разом	30	6		4	4		14
Усього	120	24		16	16		56

5. Програма навчальної дисципліни

Змістовий модуль 1. Загальні питання перетворення інформації

Основні питання:

- Зв’язок інформації з параметрами сигналів
- Квантування и дискретизація. Цифрова обробка інформації
- Види інформаційних каналів, їх математичні моделі і характеристики
- Дослідження методів цифрової обробка інформації
- Дослідження математичних моделей інформаційних каналів

Змістовий модуль 2. Принципи та методи надання доступу до інформаційних ресурсів

Основні питання:

- Принципи забезпечення доступу до інформаційних ресурсів
- Методи ідентифікації і аутентифікації користувачів
- Методи контролю доступу
- Профіль безпеки стандарту ISO/IEC 15408
- Обґрунтування профілю контролю доступу

Змістовий модуль 3. Основи теорії кодування

Основні питання:

- Скінченновимірні лінійні перетворення
- Теорема про лінійну складність комбінуючого генератора
- Криптографічні властивості булевих функцій
- Матричні операції та обчислення рангу системи векторів
- Розрахунок критерію РС(2) для булевої функції від 4-х змінних
- Знаходження покриваючого співвідношення для лінійної рекуренти методом
- Обчислення нелінійності булевої функції від 3-х змінних

Змістовий модуль 4. Основні стандарти та механізми криптографічного захисту інформації

Основні питання:

- Ітеративні Геш-функції та коди автентифікації.
- Криптографічні генератори ПВП
- Протоколи ідентифікації клієнта в системі
- Відпрацювання застосування кодів МАС на прикладі режиму імітовставки ГОСТ 28147-
- Дослідження методів рандомізації ПВП
- Відпрацювання схем протоколу вручення біту
- Відпрацювання схем протоколу вручення біту на основі Геш-функції

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю:* індивідуальне опитування, фронтальне опитування, співбесіда, залік.
- *Комп'ютерного контролю:* програми - емулятори.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

		Модуль 1	Модуль 2	Модуль 3	Модуль 4

Вид діяльності студента	Максимальна к-сть балів за одиницю	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	3	3	3	3	3	3	3	3
Відвідування семінарських занять	1								
Відвідування практичних занять	1	2	2	2	2	2	2	2	2
Відвідування лабораторних занять	1	2	2	2	2	2	2	2	2
Робота на семінарському занятті	10								
Робота на практичному занятті	10	2	20	2	20	2	20	2	20
Лабораторна робота (в тому числі допуск, виконання, захист)	10	2	20	2	20	2	20	2	20
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25	1	25
Виконання ІНДЗ	30								
Разом		-	77	-	77	-	77	-	77
Максимальна кількість балів: 308									
Розрахунок коефіцієнта: 308/100=3,08									

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Загальні питання перетворення інформації		14	5
1	Цифрова обробка інформаці. Квантування и дискретизація: • виконання завдань відповідно до теми; • опрацювання фахових видань.	14	5
Змістовий модуль 2. Принципи та методи надання доступу до інформаційних ресурсів		14	5
2	Принципи та методи надання доступу до інформаційних ресурсів: • виконання завдань відповідно до теми; • опрацювання фахових видань.	14	5
Змістовий модуль 3. Основи теорії кодування		14	5
3	Скінченновимірні лінійні перетворення. Криптографічні властивості булевих функцій: • виконання завдань відповідно до теми; • опрацювання фахових видань.	14	5
Змістовий модуль 4. Основні стандарти та механізми криптографічного захисту інформації		14	5
4	Механізми криптографічного захисту інформації. Криптографічні генератори ПВП: • виконання завдань відповідно до теми; • опрацювання фахових видань.	14	5
Разом		56	20

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – тест, що складається 3 запитань.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі заліку, умовою отримання якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Орієнтовний перелік питань для самоконтролю

1. Принципи забезпечення доступу до інформаційних ресурсів.
2. Зв'язок інформації з параметрами сигналів
3. Квантування и дискретизація.
4. Цифрова обробка інформаці
5. Види інформаційних каналів,
6. Математичні моделі інформаційних каналів
7. Алгоритм RSA.
8. Теорема дискретизації Шеннона-Котельнікова
9. Модель системи передачі інформації
10. Представлення інформації. Кількість інформації.
11. Одиниці виміру інформації. Способи вимірювання інформації
12. Види ентропії. Властивості ентропії
13. Швидкість передачі інформації
14. Перепускна здатність дискретного каналу
15. Теорема про кодування дискретного джерела
16. Стиснення інформації
17. Основні методи стиснення інформації
18. Арифметичне кодування
19. Словниково-орієнтовані алгоритми стиснення інформації
20. Стиснення інформації з втратами
21. Завадозахищене кодування
22. Математична модель системи зв'язку
23. Матричне кодування
24. Поліноміальне кодування
25. Циклічні коди
26. Коди Хеммінга
27. Адаптивні алгоритми стиснення інформації

28. Поліграмні шифри. Шифр Playfair.
29. Омофонічні шифри.
30. Шифриперестановки.
31. Шифри гамування.
32. Шифрування з відкритим ключем. Алгоритм RSA.
33. Алгоритм на основі завдання про укладання ранця.
34. Алгоритм шифрування Ель-Гамаля.
35. Алгоритм на основі еліптичних кривих.
36. Криптографічні протоколи. Хеш-функції.
37. Ітеративні Геш-функції та коди автентифікації.
38. Криптографічні генератори ПВП
39. Протоколи ідентифікації клієнта в системі
40. Застосування кодів MAC на прикладі режиму імітовставки ГОСТ 28147
41. Методи рандомізації ПВП
42. Схеми протоколу вручення біту
43. Схеми протоколу вручення біту на основі Геш-функції
44. Скінченновимірні лінійні перетворення
45. Теорема про лінійну складність комбінуючого генератора
46. Криптографічні властивості булевих функцій
47. Матричні операції та обчислення рангу системи векторів
48. Розрахунок критерію РС(2) для булевої функції від 4-х змінних
49. Знаходження покриваючого співвідношення для лінійної рекуренти методом
50. Обчислення нелінійності булевої функції від 3-х змінних
51. Принципи забезпечення доступу до інформаційних ресурсів
52. Методи ідентифікації і аутентифікації користувачів
53. Методи контролю доступу
54. Профіль безпеки стандарту ISO/IEC 15408
55. Обґрунтування профілю контролю доступу
56. Зв’язок інформації з параметрами сигналів
57. Квантування и дискретизація. Цифрова обробка інформації
58. Види інформаційних каналів, їх математичні моделі і характеристики
59. Дослідження методів цифрової обробка інформації
60. Дослідження математичних моделей інформаційних каналів

Шкала відповідності оцінок

Рейтингова оцінка	**Сума балів за всі види навчальної діяльності**	**Значення оцінки**
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов’язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов’язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов’язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 150 год., лекції – 24 год., практичні заняття – 16 год., лабораторні роботи – 16 год., модульний контроль –8 год., самостійна робота –56 год.

Модулі (назви, бали)	**Змістовий модуль 1. Загальні питання перетворення інформації (77 балів)**			**Змістовий модуль 2. Принципи та методи надання доступу до інформаційних ресурсів (77 балів)**		
Лекції (теми, бали)	Зв'язок інформації з параметрами сигналів (1 бал)	Квантування и дискретизація. Цифрова обробка інформації (1 бал)	Види інформаційних каналів, їх математичні моделі і характеристики (1 бал)	Принципи забезпечення доступу до інформаційних ресурсів (1 бал)	Методи ідентифікації і аутентифікації користувачів (1 бал)	Методи контролю доступу (1 бал)
Практичні, семінарські заняття (теми, бали)		Дослідження методів цифрової обробка інформації (22 бали)			Профіль безпеки стандарту ISO/IEC 15408 (22 бали)	
Лабораторні заняття (теми, бали)			Дослідження математичних моделей інформаційних каналів (22 бали)			Обґрунтування профілю контролю доступу (22 бали)
Самостійна робота	Самостійна робота (5 балів)			Самостійна робота (5 балів)		
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)			Модульна контрольна робота 2 (25 балів)		

Модулі (назви, бали)	**Змістовий модуль 3. Основи теорії кодування (77 балів)**			**Змістовий модуль 4. Основні стандарти та механізми криптографічного захисту інформації (77 балів)**		
Лекції (теми, бали)	Скінченновимірні лінійні перетворення (1 бал)	Теорема про лінійну складність комбінуючого генератора. (1 бал)	Криптографічні властивості булевих функцій (1 бал)	Ітеративні Геш-функції та коди автентифікації. (1 бал)	Криптографічні генератори ПВП (1 бал)	Протоколи ідентифікації клієнта в системі (1 бал)
Практичні, семінарські заняття (теми, бали)	Матричні операції та обчислення рангу системи векторів. (11 балів)		Розрахунок критерію РС(2) для булевої функції від 4-х змінних (11 балів)	Відпрацювання застосування кодів МАС на прикладі режиму імітовставки ГОСТ 28147-89 (11 балів)	Дослідження методів рандомізації ПВП (11 балів)	
Лабораторні заняття (теми, бали)		Знаходження покриваючого співвідношення для лінійної рекуренти методом Гауса (11 балів)	Обчислення нелінійності булевої функції від 3-х змінних. (11 балів)		Відпрацювання схем протоколу вручення біту (11 балів)	Відпрацювання схем протоколу вручення біту на основі Геш-функції (11 балів)
Самостійна робота	Самостійна робота (5 балів)			Самостійна робота (5 балів)		
Поточний контроль (вид, бали)	Модульна контрольна робота 3 (25 балів)			Модульна контрольна робота 4 (25 балів)		
Підсумковий контроль (вид, бали)				Залік		

8. Рекомендовані джерела

Основна (базова):

1. Манаев Е. И. Основы радиоэлектроники. – М. : Связь, 1985. – 488 с.
2. Остапенко Г. С. Усилительные устройства: Учебн. пособие для вузов. – М. : Радио и связь, 1989. – 456 с.
3. Радіотехніка: Енциклопедичний навчальний довідник: Навч. посібник / За ред. Ю.Л. Мазора, Є.А. Мачуського, В.І. Правди. – К.: Вища шк., 1999. – 838 с.
4. Прокопов І.Д. Основи систем автоматизації проектування радіоелектронних пристроїв: Навчальний посібник. –Вінниця, ВНТУ, 2006.-100с.
5. Барась С.Т., Лободзінська Р.Ф., Лазарєв О.О. Конструювання радіоелектронних засобів телекомунікаційних систем. Навчальний посібник. –Вінниця: ВНТУ, 2004.-82с.
6. Бакулев П.А., Радиолокационные системы. Учебник для вузов. – М.: Радіотехніка. 2004, 320с., ил.
7. Кузьмин И.В. Основы теории информации кодирования: учебник для вузов / И.В. Кузьмин, В.А. Кедрус . ─ 2-е изд., перераб. и доп. ─ К.: Вища школа, 1986 . ─ 237с.
8. Антенно-фидерные устройства и распространение радиоволн: Учебник для Вузов /Г.А.Ерохин, О.В.Чернышев, Н.Д,Козырев, В.Г.Кочержевский; под ред. Г.А.Ерохина. – 2-е изд., испр. – М.: Горячая линия – Телеком, 2004.- 491с.
9. В. Столингс Основы защиты сетей. Приложения и стандарты. - М.: Издательский дом «Вильямс», 2002. – 432с.
10. Волочій Б.Ю. Передавання сигналів у інформаційних системах. Частина 1. – Львів: Видавництво Національного університету “Львівська політехніка”, 2005. – 194 с.
11. Мандзій Б.А., Желяк Р.І. Основи теорії сигналів. – Львів: НВП «НОВИЙ ТЕЗАУРУС», 2001. – 152 с.
12. Андреев А. Б., Зоряев А. В. и др. Защита информации в телекоммуникационных системах: Учебник. – Воронеж: Воронежский институт МВД России, 2002. – 300 с.
13. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: ТРИУМФ, 2002. – 816 с.
14. Саломаа С. Криптографія з відкритим ключем. - Мир, 1995. - 318 с.
15. Фомичев В.М. Дискретная математика и криптология. Курс лекций. -М., Диалог-МИФИ, 2003. - 400 с.
16. Деднев М.А., Дыльнов Д.В., Иванов М.А. Зашита информации в банковском деле и электронном бизнесе. – М.: КУДИЦ-ОБРАЗ, 2004. -512с.
17. Мухачов В.А., Хорошко В.А. Методы практической криптографии. К.: ООО «ПолиграфКонсалтинг» , 2005. – 215 с.
18. Математические и компьютерные основы криптологии: Учеб. пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн.: Новое знание, 2003. – 382с.
19. Горбатов В.С., Полянская О.Ю. Основы технологии PKI – М.: Горячая линия – Телеком, 2004. – 248с..
20. Введение в криптографию / Под общ. Ред. В.В. Ященко.- 2-е изд., испр. – М.:МЦНМО:”ЧеРо”, 1999. – 271 с.
21. Вербицький О.В. Вступ до криптології. – Лв.:ВНТЛ, 1998. – 247 с.
22. Т.В. Кузьминов. Криптографические методы защиты информации. Новосибирск, «Наука», Сибирское предприятие РАН 1998. -185 с.
23. Б. Шнайер Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Изд-во ТРИУМФ,2002. – 816 с.
24. Мао, Венбо. Современная криптография: теория и практика. : Пер. С англ. – М.: Издательский дом «Вильямс», 2005. – 768 с.
25. Виноградов И. М. Основы теории чисел. —9-е изд., перераб. —М.: Наука, 1981.
26. Ф.Р. Гантмахер Теория матриц. – М.: «Наука», 1966. – 576с.
27. Кузнецов Г.В., Фомичов В.В., Сушко С.О., Фомичова Л.Я. Математичі основи

криптографі: навчальний посібник. – Дніпропетровськ: Національний гірничий університет, 2004. –ч.1. -391 с.

28. Богуш В.М., Мухачов В.А. Криптографічні застосування елементарної теорії чисел. К.: вид. ДУІКТ, 2006. – 126с.

29. Хорошко В.О. та співавтори. Компь'ютерна криптография. Лабораторний практикум. – Київ: НАУ, 2003. -94 с.

30. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых. - К.: ІВЦ Видавництво «Політехніка», 2004. – 224 с.

31. Тилборг ван Х.К.А. Основы криптологии.- .: Мир, 2006. - 471 с.

Додаткова

1. Сазонов Д.М. Антенны и устройства СВЧ: Учебник для радиотехнич. спец. вузов.- М.: Высш. шк., 1988.- 432 с.

2. Волочій Б.Ю., Озірковський Л.Д. Практикум теорії електрозв'язку. – Львів: Вид-во Національного університету "Львівська політехніка", 2010. – 116 с.

3. Дорохов А.П. Расчет и конструирование антенно-фидерных устройств. - Харьков, ХГУ, 1960, - 450с.

4. Кочержевский Г.Н. Антенно-фидерные устройства: Учебник для вузов. М., «Радио и связь», 1981. -280с.

5. Ільницкий Л.Я., Савченко А.Я., Сібрук Л.В. Антени та пристрої надвисоких частот: підручник для ВНЗ Київ: Укртелеком, 2003 р. – 496 с.

6. Рябко В. Г., Фионов А. Н. «Криптографические методы защиты информации: Учебное пособие для ВУЗов.» -М.: Горячая линия. – Телеком, 2005. – 225 с.

7. Х.К.А.ван Тилборг Основы Криптологии. Профессиональное руководство и интерактивный учебник. - М., Мир, 2006. - 471 с.

8. Математичні основи криптографії: Навч. посібник / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова. - Дніпропетровськ: Національний гірничий університет, 2004. - Ч1. - 391 с.

9. Математичні основи криптографії: конспект лекцій / викладачі: В. А. Фільштінський, А. В. Бережний. – Суми: Сумський державний університет, 2011. – 138 с.

10. ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. - М.: Изд-во стандартов, 1989. - 26 с.

11. ДСТУ 4145-2002. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих.- К.: ДКУ з питань ТР СП, 2003. – 31 с.

12. ГОСТ Р 34.10.94 Информационная технология. Криптографическая защита информации. Цифровая подпись на базе асимметричного криптографического алгоритма. – Введ. 01.01.95. – М.: Изд-во стандартов, 1994.

13. ГОСТ Р 34.311-95 Информационная технология. Криптографическая защита информации. Функция хэширования. Мн.: Межгос. Совет по стандартизации, метрологии и сертификации, 1998. -14с.

9. Додаткові ресурси

1. ISO/IEC 14888-3 Information technology - Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based Mechanisms. June 2006.

2. ISO/IEC 11770-3 Information Technology - Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques. January 2007.

3. ITU-T Recommendation X.509. Information Technology - Open Systems Interconnection - The Directory Public Key and Attribute Certificate.

4. Наказ Державного комітету України з питань регуляторної політики та підприємництва, Департаменту спеціальних телекомунікацій-них систем та захисту інформації

СБ України 29.12.2000 №88/66.

5. Положення про порядок здійснення криптографічного захисту інформації в Україні УП №505/98 від 22.05.98.

6. Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації, затверджене наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 22.10.1999 №53.

7. Тимчасова інструкція про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затверджена спільним наказом Держстандарту України та Служби безпеки України від 28.11.97 №708/156 і зареєстрована в Міністерстві юстиції України 17.12.97 за №8598/2402.

8. Andreas D. Bovopoulos and Micha Zeiger. Shared-Memory Fabrics Meet 10-Gbit Backplane Demands. TeraChip, Inc. [электронный ресурс] http://www.commsdesign.com

9. Matching Output Queueing with a Combined Input Output Queued Switch [электронный ресурс] http://www-rcf.usc.edu

10. An improved algorithm for CIOQ switches. Yossi Azar, Ybssi Richter. [электронный ресурс] http://portal.acm.org

11. Сайт научной базы данных «SciVerse ScienceDirect» [электронный ре-сурс] http://www.sciencedirect.com

12. Сайт Института инженеров по электротехнике и электронике (IEEE, Institute of Electrical and Electronics Engineers) [электронный ресурс] http://www.ieee.org